Medical Image Compression and Encryption using Chaos based DNA Cryptography

Prema T.Akkasaligar
Department of Computer Science and Engineering
B.L.D.E.A's V.P. Dr. P.G.Halakatti
College of Engineering and Technology
(Affilitaed to Visvesvaraya Technological University,
Belagavi-590018)
Vijayapur-586103, Karnataka,India
premasb@rediffmail.com

Sumangala Biradar
Department of Information Science and Engineering
B.L.D.E.A's V. P. Dr. P.G.Halakatti
College of Engineering and Technology
(Affilitaed to Visvesvaraya Technological University,
Belagavi-590018)
Vijayapur-586103, Karnataka,India
biradarsumangala@gmail.com

***Abstract*—In digital communication, the transmission of medical images over communication network is very explosive. We need a communication system to transmit the medical information rapidly and securely. In this manuscript, we propose a cryptosystem with novel encoding strategy and lossless compression technique. The chaos based DNA cryptography is used to enrich security of medical images. The lossless Discrete Haar Wavelet Transform is used to reduce space and time efficiency during transmission. The cryptanalysis proves that proposed cryptosystem is secure against different types of attacks. The compression ratio and pixel comparison is performed to verify the similarity of retained medical image.**

Keywords—DNA cryptography, Discrete Haar Wavelet Transform, Lossless compression, Medical image encryption

I. INTRODUCTION

The advancement in digital technologies leads to the transmission of the digital medical information over communication network. The communication channel used for transmission of information is not secure. The digital medical images are huge in size which requires large storage space. To provide security, several encoding strategies are available. These strategies are vulnerable against several attacks. The limitation in communication bandwidth and storage space, the transmission of the digital medical images in less time with less storage space and securely are big challenges.

Several reviews are carried out based on two categories, namely, encryption with compression methods and encryption without compression methods. In [1], discrete cosine transformation dictionary is used to compress image and hyper chaotic map is used for encryption. In [2], image is compressed using discrete cosine transform spectrum cutting method. The random matrix is created by hyper chaotic map. The discrete fractional random transform is used to encrypt the compressed random matrix. In [3], original image is compressed using 2D compressive sensing method. Further, compressed matrix pixels are shifted repeatedly using high dimensional chaotic system to attain encrypted image. In [4], sine-map, chebeychew and logistic map are used to attain linear-nonlinear-linear based structure. This structure is applied to rearrange the pixels of the image and to generate encoded image. The above discussed methods reduces time and space efficiency. But, do not resist against dictionary attack and chosen plain text attack due to less key space.

In [5], the tent map chaotic sequences are used to attain the random matrix. The logistic map is used to select DNA encoding rules. These rules are applied to medical image and plain key image to construct DNA structures. The DNA structures of the medical image and plain key image are combined using DNA algebraic operations. The outcome of this is decoded using DNA decoding rules to obtain the encrypted medical image. In [6], the patient information is concealed in the Least Signification Bit of the patient medical image. The Henon, Sin and Ten map (HST) are used to obtain pseudorandom sequences and DNA coding rules are applied to get cipher image. In [7], a 2D Logistic Adjusted Sine Map (2D-LASM) is applied to create a random matrix. This matrix is padded to the surrounding of medical image. The pixels of medical image are scrambled by 3D logistic sequences. In [8], 3D Lorenz chaotic system, DNA rules and BITXOR operations are used for diffusion, permutation, confusion and encoding of color Digital Imaging and Communication in Medicine (DICOM) images. The methods discussed in [5-8] reveals that, these methods provide high-level security but computational cost and time complexity is more.

To reduce time and space efficiency and to provide high-level security, in this manuscript we proposed a new method. In proposed method, the Discrete Haar Wavelet Transform is used to compress the medical image and further encryption is performed using chaos based DNA cryptography.

The manuscript is structured as follows: Section II explains about preliminaries for compression and encryption of medical images. Section III explains about proposed cryptosystem and Section IV about experimental results. Section V presents the conclusion.

II. PRELIMINARIES

In the proposed system, to compress the medical image lossless Discrete Haar Wavelet Transform is used. For confusion and diffusion purpose 4D Lornez chaotic map system is proposed. The DNA cryptography is used to get unique DNA structure for medical images.

A. Discrete Haar Wavelet Transform (DHWT)

The medical image contains very sensitive information about diseases of the patient. Hence, lossless compression is necessary to retrieve the original image after decompressing. The discrete haar wavelet transform is an effective method for lossless compression.

In this method, wavelet transform is applied to medical image. The transform divides image into two bands namely L and H. These bands are transformed through a series of low pass filter and high pass filter. In low pass filtering, the average operation is performed to extract the coarse coefficients from the sub bands. In high pass filtering, the

The research work is carried under the financial assistance of Vision Group of Science and Technology, Government of Karnataka, under Research Scheme for Scientists/Faculty (RGS/F) GRD No.851/315, in the year 2019-2020.

978-1-7281-6828-9/20/$31.00 ©2020 IEEE

Authorized licensed use limited to: Carleton University. Downloaded on May 28,2021 at 22:59:22 UTC from IEEE Xplore. Restrictions apply.

subtraction is performed to extract the detail coefficients from the sub bands. The output of these filters are decimated by two. Next, once again outputs are split into four bands namely, LL, HL, LH, and HH. This procedure is repeated for the whole image.

To compress the medical image, the medical image is transformed to signals. These signals are disintegrated into sequence of wavelet coefficients. The coefficients close to zero or zero are modified through threshold. Later, the modified coefficients are compressed using hamming entropy coding. In this way it compresses the medical image and decompression is the reverse process of compression.

B. 4D Lornez chaotic map

The 4D Lorenz chaotic map has unpredictable confusion and diffusion property and complex randomness. The 4D Lornez chaotic map is defined in (1) - (4):

$$x = a(y_0 - x_0) - ew_0 \quad (1)$$

$$y = x_0 z_0 - h y_0 \quad (2)$$

$$z = b - x_0 y_0 - c z_0 \quad (3)$$

$$w = k y_0 - d w_0 \quad (4)$$

where x_0, y_0, z_0 and w_0 are nonlinear deterministic state parameters and a, b, c, d, e, h are control variables.

C. DNA cryptography

DNA cryptography is a new method in cryptography. Due to uniqueness of DNA structure, it is used in proposed system. The unique DNA structure is formed by four nucleotides namely, Cytosine (C), Adenine (A), Guanine, and Thymine (T). In binary form 00 and 11, 01 and 10 are complement. In the similar way, A and T, G and C are complement. Based on this, eight DNA coding rules shown in Table I are used to generate the DNA structure.

TABLE I. DNA CODING RULES

	R1	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**
C	00	11	01	10	00	11	01	10
A	01	01	00	00	10	10	11	11
G	11	00	10	01	11	00	10	01
T	10	10	11	11	01	01	00	00

The DNA XOR method shown in Table II is used to modify the DNA structure by combing nucleotides.

TABLE II. DNA XOR OPERATION

	C	**A**	**G**	**T**
C	A	C	C	G
A	C	A	G	T
G	T	G	A	C
T	G	T	T	A

III. PROPOSED CRYPTOSYSTEM

In proposed cryptosystem, to reduce time and space efficiency during transmission the medical image is compressed. The compressed medical image pixels are scrambled and unique DNA structure is constructed to enhance the security.

The original medical image of size 512 × 512 is compressed using lossless discrete haar wavelet transform. The compressed medical image is renovated into binary image. The binary image is partitioned into 4 sub images I_1, I_2, I_3 and I_4 of size 256 × 256 each. The chaotic sequences x,

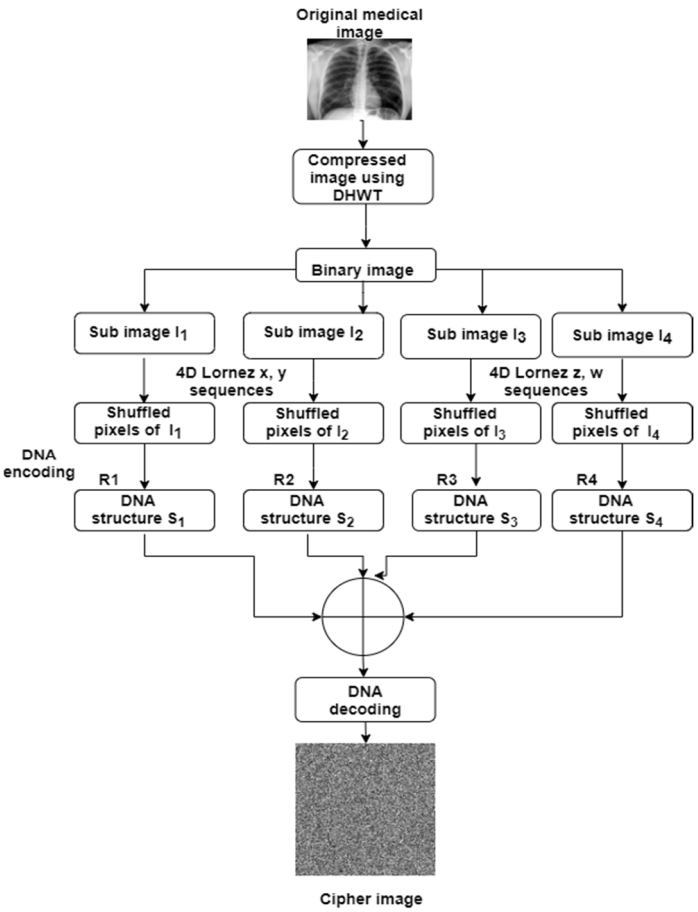

Fig. 1. Proposed system encryption process

Authorized licensed use limited to: Carleton University. Downloaded on May 28,2021 at 22:59:22 UTC from IEEE Xplore. Restrictions apply.

y, z, and w are acquired using 4D Lornez chaotic map. The chaotic sequences x and y are applied to scuffle the pixels of sub images I_1 and I_2. The chaotic sequences z and w are applied to scuffle the pixels of sub images I_3 and I_4. The DNA coding rule R1 is used for sub image I_1 and rule R3 for sub image I_3, to construct the unique DNA structure for each sub images. In the similar way, DNA coding rule R2 is used for sub image I_2 and rule R4 for sub image I_4, to construct the unique DNA structure for each sub images. The DNA structures of four sub images are combined using DNA XOR operation. The DNA complementary rules are applied to decode the combined DNA structure to get the cipher image as shown in Fig. 1.

The original medical image is retained after decrypting the encoded medical image and decompression.

IV. Experimental Results

The experiment is carried out on intel Core i7, 7th Gen processor using Matlab R2015b tool. The 500 data sets like MRI, CT, Ultrasound, ECG and X-Ray images of each type 100 samples are used to perform experiment. The original medical image of size 512×512 as shown in Fig. 2(a) is compressed using lossless discrete haar wavelet transform. The compressed image is renovated into binary image and partitioned into four sub images I_1, I_2, I_3 and I_4 of size 256 × 256 each respectively. The chaotic sequences x, y, z, and w are attained by the 4D Lornez chaotic map. The initial values of state variables x_0=3.2, y_0=8.5, z_0=3.6 and control parameters w_0= 2.2 and a= 5, b=20, c=1, d=0.1, k=0.1, e=20.8 and h=1 are empirically determined as shown in Eqns(1-4). The pixels of sub images I_1 and I_2 are scrambled using x and y chaotic sequences. Similarly, the pixels of sub images I_3 and I_4 are scrambled using z and w chaotic sequences. The unique DNA structures S_1, S_2, S_3 and S_4 are generated using DNA coding rules R1, R2, R3 and R4 respectively. The unique DNA structures of sub images are combined using DNA XOR operation specified in Table II. The cipher image shown in Fig. 2 (b) is obtained by applying DNA complementary rule.

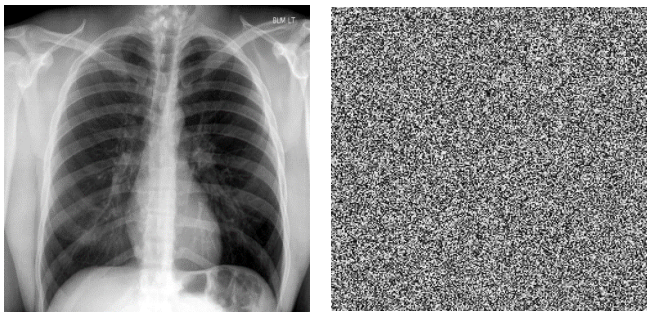

Fig. 2. (a) Original medical iamge and (b) Cipher image

The performance of the proposed cryptosystem is based on crytanalysis. The crptanalysis evaluates the propsed system by verification against statstical attack, differential attack and exhaustive attack.

A. Statstical attack

The statistical attack is the prediction of relationship by monitoring distribution of gray-level intensities in the plain image and cipher image. The histogram analysis is the graphical representation of gray-level distribution in the given image. The pixels are scattered in original medical image and pixels are uniformly distributed in cipher image. The histogram analysis of original medical image and cipher image are shown in Fig. 3 (a) and (b).

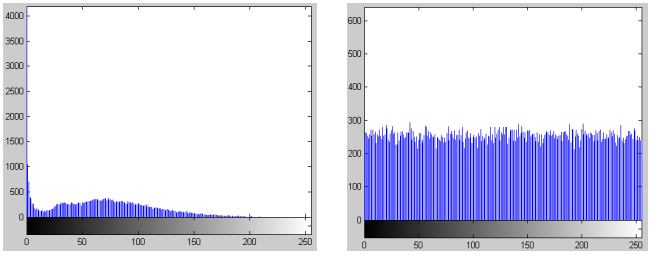

Fig. 3. Histogram of (a) Original medical iamge and (b) Cipher image

It proves that predicting the original medical image by monitoring the relationship between pixels is highly impossible.

B. Differential attack

Differential attack is to analysis the sensitivity of the original medical image related to cipher image. The small changes in the original medical image produces totally different cipher image. These changes are verified using "Number of Pixels Change Rate [NPCR]" and "Unified Average Change Intensity [UACI]".

Consider E(m, n) is the cipher image of the original image and E_1(m, n) is the cipher image of the original medical image after changing 10 pixels. The NPCR is defined in (5) and (6).

$$D_1(m,n) = \begin{cases} 0, & \text{if } E_1(m,n) = E(m,n) \\ 1, & \text{if } E_1(m,n) \neq E(m,n) \end{cases} \quad (5)$$

$$NPCR = \frac{\sum_{m,n} D_1(m,n)}{W_1 \times H_1} \times 100\% \quad (6)$$

Where W_1 is the width and H_1 is the height of the original medical image.

The UACI is defined in (7).

$$UACI = \frac{1}{W_1 \times H_1}\left[\sum_{m,n} \frac{\left|E_1(m,n) - E(m,n)\right|}{255}\right] \times 100\% \quad (7)$$

C. Exhaustive attack

Exhaustive attack is the analysis about the keys used to encode the original medical image. The exhaustive search is used to verify that, whether it is possible to guess the keys or not.

Authorized licensed use limited to: Carleton University. Downloaded on May 28,2021 at 22:59:22 UTC from IEEE Xplore. Restrictions apply.

The key space analysis is the method used by cryptanalysis to check the key length. The size of the key must be high to prevent from exhaustive attack. In proposed system, the state variables and system parameters of the 4D Lornez system are keys. The total of 10 secret keys (x_0, y_0, z_0 , w_0 a, b, c, d, e, h) are used in proposed cryptosystem. The size of the secret key is $10^{11} \times 10^{11} \times 10^{11} \times 10^{11} \times 10^{11} \times 10^{11} \times 10^{11} \times 10^{11} \times 10^{11} \times 10^{11} = 10^{110}$ if the precision is 10^{11}. The total size of secret key is very large hence the proposed cryptosystem is resist against exhaustive attack.

D. Entorpy

The entropy is a quantification of the randomness in gray-levels. The even dissemination of gray-levels indicates that the encryption method is superior. The entropy is calculated using (8).

$$E(I) = \sum_{i=1}^{n} P(O_i) \log(P(O_i)) \qquad (8)$$

where $P(O_i)$ is the probability of dissemination of grey-levels of the digital medical image and n is total number of grey-levels. The idle entropy value is 8 and proposed cryptosystem entropy value is 7.9999.

The cryptanalysis of the proposed cryptosystem is shown in Table III. The average NPCR value is 99. 92% and average UACI value is 37.68%. These values prove that proposed encryption algorithm is very sensitive against pixel change rate. The average time taken to encrypt the different types of compressed medical image is 14 seconds and decompressed image is 23 seconds. It proves that, the proposed cryptosystems time complexity is reduced. Hence, based on cryptanalysis the proposed cryptosystem is efficient and provides high-level security required for medical images.

TABLE III. CRPYTANALYSIS OF PROPOSED CRYPTO SYSTEM

Image Type	NPCR (%)	UACI (%)	Encryption Time in seconds	
			Compressed image	Decompressed image
MRI image	99.89	36.23	16	25
CT image	99.91	37.98	13	22
X-ray image	99.95	39.08	12	21
Ultrasound Image	99.89	38.95	14	23
ECG image	99.97	36.14	15	24

The compression ratio is calculated using equation (9).

$$CR = \frac{Image\ size\ after\ compression}{Image\ size\ before\ compression} \qquad (9)$$

The CR value for the proposed system on average is 7.7. To check the lossless compression, after decompression all pixels of the decompressed medical image are compared with all pixels of the original medical image.

The proposed cryptosystem is equated with the methods stated in [9-11] presented in Table IV. The NPCR, UACI and entropy value of the proposed cryptosystem is adequate to enrich the security of the medical image.

TABLE IV. COMPARSION OF PROPOSED SYSTEM

	Proposed method	[9]	[10]	[11]
NPCR	99.88	99.60	99.59	99.61
UACI	36.43	33.45	33.42	33.45
Entropy	7.9998	7.9993	7.9891	7.9992

V. CONCLUSION

In this manuscript, the original medical image is compressed using lossless discrete haar wavelet transform. The compressed image is renovated into binary image and divided into four sub images. The sub image pixels are shuffled by chaotic sequences generated using 4D Lornez chaotic map. The four unique DNA structures are constructed using DNA coding rules. The DNA structures are merged using DNA XOR operation and the cipher image is obtained after DNA decoding. The cryptanalysis proves that the proposed crypto system is secure against differential, exhaustive and statistical attacks. The proposed cryptosystem is appropriate for telemedicine and e-health applications.

REFERENCES

[1] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyperchaotic system," Nonlinear Dyn., vol. 84, no. 4, pp. 2333- 2356, Jun 2016.

[2] L Gong, C Deng, S Pan, N Zhou, "Image compression encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," Opt Laser Technol, vol.103, no.1 pp.48-58,Jul 2018 .

[3] N Zhou, S Pan, S Cheng, Z Zhou, " Image compression– encryption scheme based on hyper-chaotic system and 2D compressive sensing," Opt Laser Technol, vol.82,pp.121- 133,Aug 2016.

[4] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Process., vol. 138, pp. 129-137, Sep 2017.

[5] Dagadu, Joshua C., Jianping Li, Emelia Opoku Aboagye, and Faith K. Deynu, "Medical Image Encryption Scheme Based on Multiple Chaos and DNA Coding," IJ Network Security 21, no. 1, pp.83-90, 2019.

[6] Abdelfattah, Roayat Ismail, Hager Mohamed, and Mohamed E. Nasr. "Secure Image Encryption Scheme Based on DNA and New Multi Chaotic Map." In Journal of Physics: Conference Series, vol. 1447, no. 1, p. 012053. IOP Publishing, 2020.

[7] A Adedokun, Bello J Akan, H B Salau, I J Umoh, Richard I Nwosu, Yunusa Ibrahim, " A Secure Chaotic Framework for Medical Image Encryption using a 3D Logistic Map", Applications Of Modelling and Simulation, vol. 4, pp.141-148, 2020.

[8] Kumari, Abinaya, B. Akshaya, B. Umamaheswari, K. Thenmozhi, Rengarajan Amirtharajan, and Padmapriya Praveenkumar, "3D Lorenz Map Governs DNA Rule in Encrypting DICOM Images," Biomedical and Pharmacology ,Journal, vol. 11, no. 2, pp. 897-906, 2018.

[9] C. Fu, Y.-F. Shan, M.-Y. He, Z.-Y. Yu and H.-L. Wu, "A new medical image encryption algorithm using multiple 1-D chaotic maps," IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, pp.2055–2060, 2018.

Authorized licensed use limited to: Carleton University. Downloaded on May 28,2021 at 22:59:22 UTC from IEEE Xplore. Restrictions apply.

[10] X. Chen and C.-J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," Saudi Journal of Biological Sciences, 24(8), pp.1821–1827, 2017.

[11] Y. Chen, C. Tang and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," Signal Processing, 167, 2019.

Authorized licensed use limited to: Carleton University. Downloaded on May 28,2021 at 22:59:22 UTC from IEEE Xplore. Restrictions apply.